INTERNAL/EXTERNAL AUDIT WORKPROGRAM CHAPTER 8WP

(FILE NAME ON DISK # 3= IS-WP#03.WPD) ***COMMENTS***

The objective of this section is to determine whether there is an effective ongoing audit program. These procedures will disclose the adequacy of IS audit coverage and to what extent, if any, the examiner may rely upon the procedures performed by the auditors in determining the scope (limited or expanded) of the IS examination. Document any findings, especially those that do not satisfy the recommendations in the *1996 FFIEC IS Examination Handbook.*

BOARD SUPERVISION OF IS AUDIT

1. Review bylaws, board resolution, and audit charter to determine the authority and mission of the IS audit function.

2. Review and summarize the minutes of the board or audit committee for board member attendance and supervision of IS audit activities and determine if the board approves audit plans and schedules, reviews actual performance of plans and schedules, approves major deviations from plans, and reviews audit findings to resolution and the work of external auditors and consultants.

3. Determine if the external auditing program complements the IS internal auditing function/activities.

INDEPENDENCE AND STAFFING OF IS AUDIT

4. Determine that the reporting process for the IS audit is independent in fact and in appearance by reviewing the degree of control persons outside of the audit function have on the board or audit committee.

5. Review the internal audit organization structure for independence and clarity of the reporting process.

6. Determine that the IS audit staff is adequate in number and is technically competent to accomplish its mission.

   a. Review data sheets and evaluate IS audit personnel qualifications to the job descriptions.

b. Determine if staff competency is commensurate with the technology in use at the institution.

c. Review the IS audit budget and discuss with audit management the adequacy of current staffing levels, turnover, and staff training.

OVERALL AUDIT STANDARDS

7. Review the IS audit standards manual and/or IS related sections of the general audit manual. Assess the adequacy of policies, practices, and procedures covering the format and content of reports, distribution of reports, resolution of audit findings, format and contents of workpapers, and security over audit materials.

IS AUDIT PLANNING

8. Determine that the planning and scheduling of IS audit work are adequate to accomplish the mission of IS audit.

   a. Evaluate planning and scheduling criteria (including risk analysis) for selection, scope, and frequency of audits. Determine if:

      1) The audit universe is well defined.

      2) Audit schedules that support the entire audit universe will be reviewed within the audit cycle.

      3) The audit cycle is reasonable as approved by the board of directors .

   b. As applicable, determine the date of the last audit covering:

      1) Management

         a) Corporate Contingency Planning
         b) Management Information Systems (MIS)

      2) Systems Development and Programming.

         a) Programming Controls
         b) Acceptance and Cataloging
         c) Operating System Controls
         d) Data Base Management

e) Reviews of New Applications, Post Implementation Reviews, and Reviews of Existing Application Reviews (List Applications)

3) Operations

a) Physical/Environmental Controls
b) Data Controls
c) User Department Controls (List Departments)

4) Security - Physical and Data

a) Networks/Teleprocessing
b) Data Security
c) Physical Security

5) Networking and Client/Server

6) End User Computing (List Systems)

7) Document Imaging

8) Electronic Funds Transfer (EFT)

a) Wholesale EFT
b) Fedline EFT
c) Retail EFTs (ATM, POS, Debit Card, Home Banking)
d) Automated Clearing House (ACH)

9) Service Provider/Receiver Activities:

a) IS services provided to external users
b) IS services received from external Sources

c) Discuss with audit management significant information systems and data processing activities that have not been audited within scheduled time frames. Areas not audited within scheduled time frames, especially those not completed for an extended period, may be considered for Tier II review.

INDIVIDUAL IS AUDIT PROCEDURES

9. For each area established under IS AUDIT PLANNING (Step 8a. above), determine that the audit procedures employed meet Tier I standards as set forth in the following individual examination steps. Reference is also made to the appropriate chapter and section of this *Handbook* for additional detail supporting Tier I review procedures. Failure to meet these minimum standards may prompt a full or modified Tier II review of the area. Reference below to parts a. through h. Provide an overview of audit coverage across IS areas of activity.

   a. Determine whether audit procedures for **MANAGEMENT** adequately consider:

      1) Personnel policies, including hiring, termination, and training (training should cover awareness training for emergencies, information confidentiality, security, etc,).

      2) Job descriptions and reporting structures are current and appropriate to the job functions and the nature of the organization.

      3) Formal contracts govern activities of contract programmers and other outside consultants and include provisions that subject them to the same policies and procedures as employees.

      4) Insurance issues for consultants have been fully addressed by management.

      5) Adequacy of oversight by senior management, applicable committees, and the board of directors.

      6) Corporate contingency plans are comprehensive, current, and adequately tested.

      7) Management information systems (MIS) provide timely, accurate, consistent, complete, and relevant information.

b. Determine whether audit procedures for **SYSTEMS DEVELOPMENT AND PROGRAMMING** adequately consider:

1) Programming Controls:

a) The institution's formal application development/acquisition methodology and compliance with it.

b) Written programming standards covering coding techniques, documentation, testing, acceptance, and turnover, and compliance with the standards.

c) Segregation of duties between application program development and operating systems programming activities.

d) Program documentation library and/or quality control procedures employed to ensure adherence to systems/programming standards.

e) Controls over on-line programming terminals and access to interactive programming products.

f) Parity of production source and object files (if covered in individual application reviews, note here for cross-reference).

g) Completeness of program documentation, including history of program changes (if covered in individual application reviews, note here for cross-reference).

2) Acceptance and Cataloging Controls:

a) Separation of duties between operations, application programming, and operating systems programming during the cataloging process.

b) Parity between the approved programs and/or program changes to the cataloged version.

c) Approved programs and/or changes are controlled to prevent changes between the approval, testing, and cataloging phases.

d) That test results are properly approved and acceptance authorized before cataloging.

e) That documentation is properly updated.

f) If source code is maintained by the vendor, that an escrow agreement is in effect and the file has been confirmed as being current.

3) Operating System Controls:

a) The controls over utility programs, primarily those with production data or program file altering capabilities.

b) Separation of duties between production data file maintenance and operating system maintenance.

c) Documentation of the operating systems.

d) Controls over system documentation, vendor, and technical engineer manuals, and other sensitive operating system-related materials (access to this information should be limited to those directly responsible for maintaining the system – usually system programmers and/or technical support personnel).

e) Controls over fixes, exit routines, new releases, and other changes to the operating system.

4) Data Base Management:

a) The appointment of a data base administrator.

b) Written procedures employed, including those for maintenance of a data dictionary, and adherence to them.

c) Segregation of duties in maintaining, monitoring, and supervising data base management activities.

d) Effectiveness of transaction logs and procedures to allow recovery of the data base.

e) Data security measures employed to ensure against unauthorized access of data and/or changes to it.

5) Reviews of new applications, post implementation reviews, and review of existing systems to determine that:

a) Systems design is consistent with original objectives.

b) Programs comply with standards.

c) Audit trails and controls are satisfactory.

d) Test plans are/were satisfactory.

e) Test results are satisfactory.

f) Program documentation is adequate.

g) Program changes were reviewed and authorized properly.

h) Program changes were updated properly in documentation.

i) Source and object programs are in parity with each other.

c. Determine whether audit procedures for **OPERATIONS** adequately consider:

1) Physical/Environmental Controls:

a) Computer operations standards and procedures and compliance with them.

b) Reporting mechanisms used by data center management to monitor IS operations.

c) Equipment maintenance and records of equipment problems.

d) Controls over data processing equipment, data files, and production program libraries.

e) Segregation of duties between input, computer operations, and output.

f) Disaster prevention (fire detection, backup power, etc.).

g) Emergency procedures.

h) Housekeeping.

2) Data Controls (If these controls are reviewed by audit as part of other audits, such as computer operations, and user department controls note here for cross-reference.):

a) Evaluation of control points, using flow charts or other techniques (i.e., narratives, matrix).

b) Written procedures and compliance with them.

c) Segregation of duties between origination, input, and output.

d) Control totals generated at input are reconciled at each turnover point.

e) Adherence to formal report processing and distribution procedures.

f) Controls over negotiable and/or sensitive documents generated by the computer.

g) Control over the disposal of printed and magnetic data.

3) User Department Controls:

a) Evaluation of control points, in the user area, using flow charts or other techniques (i.e., narratives, matrix).

b) Separation of duties (input, output, reconciliation, supervision, etc.).

c) Reconcilement of computer records to the general ledger and other control figures (i.e., data entry controls to transactions listing, and hash total used to control non-financial data).

d) Report distribution and usage.

e) Record retention.

d. Determine the adequacy of audit procedures for **SECURITY-- PHYSICAL** and **DATA** for:

1) Data Security:

a) A written data security policy is in effect covering all applications employing teleprocessing systems and compliance with it.

b) Data security activities are independent from systems and programming, computer operations, data input/output, and audit.

c) Access to the systems is restricted by user identification and/or passwords.

d) Access codes are protected properly and changed with reasonable frequency.

e) Transaction files are maintained for all messages entered by terminals.

f) Unauthorized attempts to gain access to the systems are monitored by independent parties.

g) User manuals adequately describe processing requirements.

h) Controls over the telecommunications line used by vendors to maintain software.

2) Physical Security Controls:

a) Access to buildings, computer rooms, and sensitive equipment is controlled adequately.

e. Determine whether audit procedures covering reviews of **NETWORKING-CLIENT/ SERVER**:

1) Written procedures govern the activities of personnel responsible for maintaining the network.

2) The network is fully documented, including remote dial-up, with documentation available to authorized persons only.

3) Logical controls limit access to network software to authorized persons only.

4) Physical controls protect communications equipment, diagnostic equipment, and communications lines from unauthorized access.

5) Adequate network updating and testing procedures are in place.

6) Adequate approvals are required before deployment of remote terminals in homes of personnel and other dial-up locations, and such deployment is consistent with insurance provisions.

7) Alternate network communications procedures are incorporated into the disaster recovery plans.

f. If the institution employs **END-USER COMPUTING**, determine that adequate audit procedures are used to evaluate:

1) The existence of and adherence to a formal institution microcomputer policy.

2) The designation of a function to enforce policies, maintain inventory of hardware and software, and assist users to use the systems.

3) Physical and data security.

4) Data, programming, and security controls on microcomputer applications used for generating official records, making management decisions, and preparing regulatory or management reports.

5) Disaster recovery plans relative to significant microcomputer applications.

6) Software inventory check for use of unlicensed software.

g. If **ELECTRONIC FUNDS TRANSFER** (EFT) activity is performed, determine if audit procedures adequately address:

1) Wholesale EFT.

a) Adequate operating policies and procedures govern all activities, both in the wire transfer department and in the originating department, including authorization and authentication requirements, notification etc.

b) Formal contracts with each wire servicer exist, i.e., FRB, correspondent banks, and others.

c) Separation of duties are sufficient to prevent any one person from initiating, verifying, and executing a transfer of funds.

d) Personnel policies and practices are in effect.

e) Adequate security policies protect wire transfer equipment, software, communications lines, incoming and outgoing payment orders, test keys, etc.

f) Credit policies and appropriate management approvals have been established to cover overdrafts.

g) Activity reporting, monitoring, and reconcilement are conducted daily, or more frequently based upon activity.

h) Activity is covered by appropriate insurance riders.

i) Contingency plans are appropriate for the size and complexity of the wire transfer function.

j) Activity conforms with UCC 4A.

k) Funds transfer terminals are protected by adequate password security.

2) Retail EFT (ATMs, POS, Debit Cards, Home Banking).

a) Written procedures are complete and address each EFTS activity.

b) All EFTS functions are documented appropriately.

c) Physical controls protect plastic cards, PIN information, EFTS equipment, and communication systems.

d) Separation of duties and logical controls protect EFTS related software, customer account, and PIN information.

e) All transactions are properly recorded, including exception items, and constitute an acceptable audit trail for each activity.

f) Reconcilements and proofs are performed daily by persons with no conflicting duties.

g) Contingency planning is adequate.

h) Vendor and customer contracts are in effect and detail the responsibilities of all parties to the agreement.

i) Insurance coverage is adequate.

j) All EFTS activity conforms to applicable provisions of Regulation E.

3) ACH (Automated Clearing House).

a) Policies and procedures govern all ACH activity.

b) Incoming debit and credit totals are verified adequately and items counted prior to posting to customer accounts.

c) Controls over rejects, charge backs, unposted, and other suspense items are adequate.

d) Controls prevent the altering of data between receipt of data and posting to accounts.

e) Controls exist over any origination functions, including separation of data preparation, input, transmission, and reconcilement.

f) Security and control exist over ACH capture and transmission equipment.

g) Clearinghouse and FRB rules and regulations are complied with.

h. Determine whether audit procedures covering reviews of **IS SERVICE PROVIDER/ RECEIVER ACTIVITIES** address:

1) Service provider external users.

a) Formal procedures are in effect and staff is assigned to provide interface with users/customers to control data center related issues (i.e., program change requests, record differences, service quality).

b) Completeness of contracts with all customers (affiliated and nonaffiliated) and that they have been approved by the institution’s legal staff.

c) Controls over billing and income collection.

d) Disaster recovery interface between the data center and customers/users.

e) Controls over on-line terminals employed by users/customers.

f) Distribution of comprehensive user manuals.

2) IS services received from external sources.

a) Completeness of contracts and that they have been approved by the institution’s legal staff.

b) Satisfactory performance of contracted services.

c) The financial condition of the vendor.

d) Applicable emergency and disaster recovery plans are in effect.

e) Controls over the on-line terminal used by the bank to access files at an external servicer's location.

f) Internal controls for each significant user and/or new application are consistent with those required for in-house systems. (NOTE: Consider the other steps included herein and of third party audit reviews.)

10. If **AUDIT SOFTWARE** is used, obtain a summary listing that includes:

a. Program name.

b. Applications audited with this program.

c. Name of audit software vendor or author (if internally developed).

d. Frequency of use and date last used.

e. SOFTWARE that:

1) Meets the criteria detailed in Chapter 8, Audit.

2) Is appropriate for the size and complexity of the data center.

3) Contains resident programs that are secured adequately in private libraries or otherwise under the control of the auditor.

4) Has related documentation, which is secure and under the control of auditor.

5) Requires the auditor to be adequately trained to make full and effective use of the automated tools.

6) Documentation adheres to written standards for the in-house developed programs and for purchased products. (Note: Documentation standards should be consistent with those developed for the Systems and Programming function.)

Systems Development and Major Program Changes

11. Review the methodology employed to notify the IS auditor of proposed new applications, major changes to existing applications, modifications/additions to the operating system, and other changes to the data processing environment (e.g., equipment configurations, and organizational structure). Determine the adequacy of auditing in:

    a) Participating in the systems development life cycle.

    b) Reviewing major changes to applications or the operating system.

    c) Updating audit procedures, software, and documentation for changes in the systems or environment.

    d) Recommending changes to new proposals or to existing applications and systems.

Audit Reports and Documentation

12. Audit reports

a) If not included in the review of board or audit committee minutes, review reports to senior management that summarize audit activities and findings. Document any unresolved exceptions for follow-up in the applicable section of the workprogram.

b) For each IS audit performed since the last examination, complete the **IS AUDIT REPORT AND WORKPAPER REVIEW SHEET** included in this section and consistent with the scope of the examination determine the degree of examination work to be conducted during this examination (i.e., Tier I only, Tier I with follow-up of audit exceptions, or Tier I and Tier II).

c) Select a sample of workpapers sufficient to determine their consistency in supporting the satisfactory execution of audit procedures and findings. If the workpapers do not generally support audit performance or individual areas, this condition should be considered in determining the scope of review in the other section of the workprogram.

Audit Follow-up

13. Determine whether audit follow-up procedures require:

a) A written management reply addressing each deficiency, including corrective action taken.

b) Subsequent audit tests to verify the resolution of deficiencies.

c) Written reports to the board or audit committee detailing the findings of the follow-up.

External Audit

14. If IS audit coverage is provided by external auditors or outside consultants:

a) Identify the name of the CPA and/or consultant and whether any affiliate or other relationships exist.

b) Review engagement letter(s) and contract(s) to determine the scope and frequency.

c) If external sources are the primary source of audit coverage for all IS activities or specific IS areas, determine that the procedures employed meet the minimum standards set forth in the other applicable steps of this section. Review all reports by completing **IS AUDIT REPORT AND WORKPAPER REVIEW SHEET** and test workpapers to the extent deemed necessary. As applicable determine if the external audits adequately cover:

1) Management/Administration.

   a) Corporate Contingency Planning.

   b) Management Information Systems.

2) Systems and Programming.

   a) Programming Controls.

   b) Acceptance and Cataloging.

   c) Operating System Controls.

   d) Data Base Management.

   e) Application Reviews.

3) Operations.

   a) Physical/Environmental Controls.

   b) Data Controls.

   c) User Department Controls.

4) Security– Physical and Data.

   a) Data Security.

   b) Physical Security.

5) Service Provider/Receiver Activities.

   a) IS Services Provided to External Users.

   b) IS Services Received from External Users.

6) End User Computing.

7) Electronic Funds Transfer.

a) Wholesale EFT.

b) Retail EFTS (ATM, POS, Debit Card, Home Banking)

c) ACH EFT

d. If the engagement was a special review, determine the purpose and whether proper levels of management have reviewed the report. Document the findings in the report and the status of any exceptions noted. All unresolved exceptions should be followed up in the applicable sections of the workprogram.

THIRD-PARTY REVIEWS

15. If significant data processing services are provided by independent data processors, determine whether:

a) Management either employs the services of external auditors directly to evaluate the servicer's controls or requests copies from the servicer of the most recent external audit report.

b) Management requests applicable regulatory agency IS examination reports.

c) All third-party reports are reviewed adequately and followed up appropriately by the auditor.

d) The institution obtains and analyzes the vendor’s financial statements.

CONCLUSIONS

16. Assess the independence, competency, and scope of the internal/external audit function(s) to determine whether audit coverage may be relied upon in determining the scope of the IS examination by:

a) Reviewing IS AUDIT PLANNING (Step 8), INDIVIDUAL IS AUDIT PROCEDURES (Steps 9a through 9*1*) and IS AUDIT REPORT AND WORKPAPER REVIEW SHEETS to determine whether any sections or parts of other sections of the workprogram may require Tier II coverage and/or follow-up for resolution of audit exceptions. Cross-reference with applicable sections to ensure performance.

b) Assessing, audits compliance with Part 363 of the FDIC Rules and Regulations and Statement of Policies 12-28-88 and 1-16-90.

17. Discuss with management:

a) Violations of law, rulings, regulations or significant internal control deficiencies.

b) Recommended corrective action for deficiencies cited.

c) Management's proposed actions for correcting deficiencies.

18. Assign rating. (See Chapter 5 for additional information.)

19. Prepare an index of workpapers for this section of the workprogram.

20. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include important facts, findings, examiner conclusions, and, if applicable, recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations.

21. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.

Examiner | Date

_________|________

Reviewer's Initials

SUMMARY OF EXCEPTIONS

List significant exceptions for follow-up and discussion as determined through the review of audit reports and/or the examination procedures.

Section Name:

IS AUDIT REPORT AND WORK PAPER REVIEW SHEET

(Make additional copies for each audit reviewed.

Name of Institution:	Date of IS Exam:
Report Name:	Auditor's Name:
Prior Audit Date:	Audit Rating:
Audit Date:	Report Date:
Management Response Date:	Follow-up Date:

1. Is the report:

   a. In compliance with the standard format?

   b. Logical, effective, and understandable?

   c. Adequate in describing the scope and objectives?

   d. Adequate in describing significant deficiencies?

   e. Adequate in suggesting corrective measures?

   f. Clear in stating the auditor’s opinion/conclusion about the condition and effectiveness of controls in the audited area? Was a rating assigned?

2. Were the objectives reasonable and sufficient?

3. Did management respond:

   a. To the exceptions in a positive manner?

   b. In a timely manner?

   c. With a date of corrective action?

4. Did the auditor:

   a. Review the responses for completeness?

   b. Perform or schedule a follow-up audit?

5. Have the deficiencies been resolved?

6. If workpapers for this area were tested, are they:

   a. Adequate in content to determine that audit procedures have been carried out?

   b. Filed in a uniform manner?

   c. Adequately safeguarded?

Name of Institution:

BIOGRAPHICAL DATA WORKSHEET

PERSONAL

(Name) ____ (Birth Date) ___________________

(Title) ____

(Responsibilities) ____

____

____

(Years with Bank/Center) ____________________ (Years in Present Position) ________________

(Previous Position) ____

(Responsibilities) ____

If employed by bank/center less than two years, provide the following:

(Previous Employer) ________________________________ (Years with that Employer) __________

(Highest Position Attained) ____

(Responsibilities) ____

PROFESSIONAL

(EDUCATION): High School _____ College _____ Bus. College _____
Major Field ____________________Degree______________
(Indicate number years attended or degree.)

(Continuing Education):

Seminar/Course Title **Presented by** **Dates attended**

1. ___________________________________ ______________________________ _________________
2. ___________________________________ ______________________________ _________________
3. ___________________________________ ______________________________ _________________
4. ___________________________________ ______________________________ _________________
5. ___________________________________ ______________________________ _________________
6. ___________________________________ ______________________________ _________________
7. ___________________________________ ______________________________ _________________
8. ___________________________________ ______________________________ _________________
9. ___________________________________ ______________________________ _________________
10. ___________________________________ ______________________________ _________________

(Membership in Business/Professional Organizations)

1. ____
2. ____
3. ____

Exhibit No. ____________________
Date________________________
Prepared By____________________